

(51) Int. Cl. ⁷	識別記号	F I	ターマコード [*] (参考)
G06F 12/14	320	G06F 12/14	320 B 5B017
12/00	537	12/00	537 H 5B082
G09C 1/00	660	G09C 1/00	660 D 5J104

審査請求 未請求 請求項の数 5 O L (全19頁)

(21) 出願番号 特願2001-327302(P 2001-327302)

(22) 出願日 平成13年10月25日(2001.10.25)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(72) 発明者 安孫子 幸弘

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72) 発明者 岡田 佳之

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(74) 代理人 100092978

弁理士 真田 有

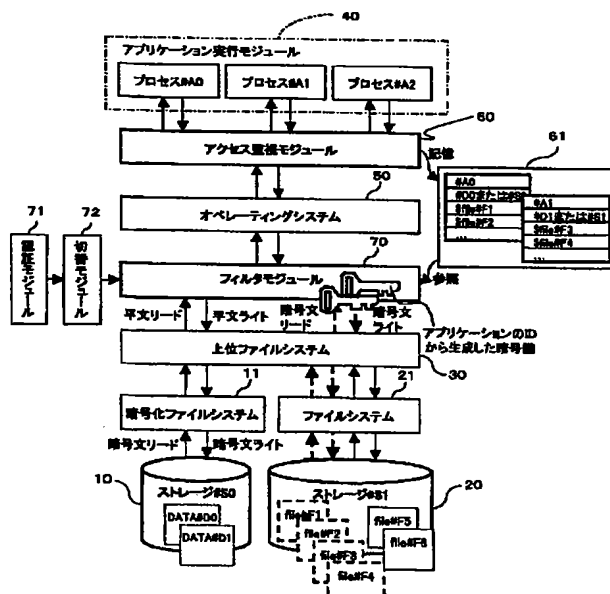
最終頁に続く

(54) 【発明の名称】 データ管理システム

(57) 【要約】

【課題】 暗号化機能なしの蓄積媒体と暗号化機能ありの蓄積媒体とを混在させて使用する状況であっても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護できるようにする。

【解決手段】 コンテンツを蓄積する蓄積媒体10、20と、アプリケーション実行手段40と、このアプリケーション実行手段で動作中のアプリケーションの固有情報とアプリケーションがアクセスしているコンテンツの固有情報とを対応付けてアクセス状況を監視するアクセス監視手段60と、動作中のアプリケーションがコンテンツを蓄積媒体20に書き込む際にはアプリケーションの固有情報を用いてコンテンツを暗号化する一方、動作中のアプリケーションがコンテンツを蓄積媒体20から読み出す際にはアプリケーションの固有情報を用いてコンテンツを復号化するフィルタリング手段70とをそなえて構成する。



【特許請求の範囲】

【請求項 1】 コンテンツを蓄積する蓄積媒体と、
該蓄積媒体における該コンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、
該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、
動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴とする、データ管理システム。

【請求項 2】 該アプリケーションの実行を制御するソフトウェアとしてのオペレーティングシステムをさらにそなえ、

該アクセス監視手段が、該アプリケーションについての固有情報として、該アプリケーション実行手段が該アプリケーションを実行する際に該オペレーティングシステムから与えられるプロセス毎の識別情報を用いることを特徴とする、請求項 1 記載のデータ管理システム。

【請求項 3】 該アクセス監視手段が、該アプリケーションについての固有情報と該コンテンツについての固有情報とを対応付けて管理テーブルに登録し、該管理テーブルを用いて該アクセス状況を監視することを特徴とする、請求項 1 または請求項 2 に記載のデータ管理システム。

【請求項 4】 該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、
該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、
該ファイルシステムのうちの少なくとも一つが、該コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有し該ファイル毎または該フォルダ毎に暗号化を行なった上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、請求項 3 記載のデータ管理システム。

【請求項 5】 該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、
該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、
該ファイルシステムのうちの少なくとも一つが、そのファイルシステムの全体を暗号化した上で該コンテンツを

該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、請求項 3 記載のデータ管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、例えば、ハードディスクレコーダ等の記録再生装置やパーソナルコンピュータ等のデータ処理装置を含んで構成されるシステムにおいて、各種デジタルコンテンツの著作権を保護するための技術に関する。

【0002】

【従来の技術】 近年、デジタル化技術の発展とストレージ装置の大容量化、そしてネットワークの広帯域化に伴い、映像データ（動画データ）や音声データあるいは画像データなどを含むコンテンツは、デジタル化後にストレージ装置や可換媒体などの各種記録媒体に蓄積され、ネットワークや可換媒体を介して容易に交換されるようになりつつある。

【0003】 しかし、データの交換が容易になることによって、ユーザは、無意識のうちにあるいは故意に、コンテンツの作者の許諾なしにデータを配布したり譲渡したりして、著作権を侵害してしまうケースが増加している。そこで、これまでに著作権を保護すべく、著作物を暗号化する技術が開発されてきている。このような技術を導入すると、暗号鍵を手でできない限り、暗号化されたデータ（以下、暗号化データという）は意味をなさないため、暗号化は著作権保護に有効である。

【0004】 ところが、暗号化データをアプリケーションが利用するためには、その暗号化データを復号化して記録媒体に蓄積する必要がある。このように復号化されたデータが、一旦、記録媒体に蓄積された後は、データの移動、複写、改竄などの処理を自由に行なえるようになってしまうので、著作権保護機能が働かなくなることが懸念される。

【0005】 このような状況に対応すべく、従来、例えば特開 2000-311114 号公報や特開 2000-330870 号公報などに開示されるような技術が提案されている。これらの公報に開示された技術では、可換媒体を用いる場合、データを暗号化の際に、媒体固有のメディア ID (IDentification) が暗号鍵として用いられる。メディア ID を持たない媒体に対しては、ファイルシステムから通常アクセスできないリードイン領域、交替処理領域、ROM (Read Only Memory) 領域に書かれる暗号鍵が用いられる。また、ハードディスク装置のように通常特別な ROM 領域を持たない媒体に対しては、BIOS (Basic Input Output System) によって隠蔽されたデバイス ID が暗号鍵として用いられる。上述した公報に開示された技術では、これらの暗号鍵によって暗号化されたデータを各媒体に蓄積することによって、著作権が保護されている。

【0006】

【発明が解決しようとする課題】ところで、既に著作権保護機能なしに運用されているパーソナルコンピュータやデータ記録再生装置などのシステムに、暗号化された著作物（コンテンツ）を含む蓄積媒体を後付けして使用した場合などには、暗号化機能なしの蓄積媒体（暗号化する必要のないデータを蓄積するハードディスク）と暗号化機能ありの蓄積媒体（暗号化データを蓄積するハードディスク）とを混在させて使用する状況が発生する。

【0007】このような状況下において、アプリケーションが暗号化データを読み出して使用すると、暗号化が解除された著作物データの全部もしくは一部が流通されてしまうことになる。上述した従来技術では、このような状況での著作権保護対策は何ら開示されていない。

【0008】例えば、編集アプリケーションを利用してデータに変更を加える場合に、中間処理結果をファイルに一時的に保存したりメモリファイルに一時的に蓄積したりする状況を想定する。すると、著作物として意味のある内容を持つ一時蓄積ファイルが、暗号化の対象としている媒体以外において生成され、暗号化されていないデータとして保存されることになる。従って、既存のファイルシステムを用いて、著作権を保護するためのシステムを構築しようすると、ハードディスク内のデータを全て暗号化する変換作業が求められることになる。しかし、このようなシステムを構築すると、著作者あるいは著作者から許諾を受けている者に対して、著作権の行使が著しく制限されてしまうため、逆に著作権が侵害されてしまう。

【0009】本発明は、このような課題に鑑み創案されたもので、暗号化機能なしの蓄積媒体と暗号化機能ありの蓄積媒体とを混在させて使用する状況であっても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護できるようにすることを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明のデータ管理システム（請求項1）は、コンテンツを蓄積する蓄積媒体と、該蓄積媒体における該コンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該

コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴としている。

【0011】なお、該アプリケーションの実行を制御するソフトウェアとしてのオペレーティングシステムをさらにそなえ、該アクセス監視手段が、該アプリケーションについての固有情報として、該アプリケーション実行手段が該アプリケーションを実行する際に該オペレーティングシステムから与えられるプロセス毎の識別情報を用いるように構成してもよい（請求項2）。

【0012】また、該アクセス監視手段が、該アプリケーションについての固有情報と該コンテンツについての固有情報とを対応付けて管理テーブルに登録し、該管理テーブルを用いて該アクセス状況を監視するように構成してもよい（請求項3）。

【0013】このとき、該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、該ファイルシステムのうちの少なくとも一つが、該コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有し該ファイル毎または該フォルダ毎に暗号化を行なった上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステム（請求項4）、もしくは、そのファイルシステムの全体を暗号化した上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステム（請求項5）であってもよい。

【0014】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

〔1〕第1実施形態の説明

図1は本発明の第1実施形態としてのデータ管理システムの構成を示すブロック図であり、この図1に示すように、第1実施形態のデータ管理システムは、例えば汎用のパーソナルコンピュータ（データ処理装置）に組み込まれたもので、ストレージ10、暗号化ファイルシステム11、ストレージ20、ファイルシステム21、上位ファイルシステム30、アプリケーション実行モジュール40、オペレーティングシステム50、アクセス監視モジュール60、フィルタモジュール70、認証モジュール71および切替モジュール72をそなえて構成されている。

【0015】第1実施形態のデータ管理システムには、2つのストレージ10および20がそなえられており、各ストレージ10、20に一つの論理ドライブが構築されている。なお、図1に示す例では、ストレージ10、20にそれぞれ構築された論理ドライブのドライブ名を#S0、#S1としている。

【0016】ストレージ10は、後述する暗号化ファイルシステム11で管理される論理ドライブを含む第1蓄積装置（暗号化機能ありの蓄積媒体）として機能するも

のである。暗号化ファイルシステム11は、コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有しファイル毎またはフォルダ毎に暗号化を行なった上でコンテンツ（著作物ファイル）をストレージ10に蓄積させるもの、もしくは、そのファイルシステムの全体を暗号化した上でコンテンツ（著作物ファイル）をストレージ10に蓄積させるものである。

【0017】従って、ストレージ10の論理ドライブにデータを書き込むと、そのデータは、暗号化ファイルシステム11によって暗号化されてから書き込まれる一方、ストレージ10の論理ドライブから暗号化データを読み出すと、その暗号化データは、暗号化ファイルシステム11によって復号化されてから読み出されるようになっている。なお、図1では、ストレージ10に、暗号化された2つの著作物ファイル（ファイル名#D0、#D1）を蓄積した例が示されている。

【0018】ストレージ20は、後述するフィルタモジュール70によって暗号化されたコンテンツを蓄積する第2蓄積装置（暗号化機能なしの蓄積媒体）として機能するものである。このストレージ20に構築された論理ドライブは、例えばFAT（File Allocation Table）等のファイルシステム21によって管理されている。なお、図1では、ストレージ20に、暗号化された4つのファイル（ファイル名#F1～#F4）と暗号化されていない2つのファイル（ファイル名#F5、#F6）とを蓄積した例が示されている。

【0019】上位ファイルシステム30は、暗号化ファイルシステム11およびファイルシステム21の両方を管理するもので、これらのファイルシステム11、12と後述するフィルタモジュール70との間に介在するものである。アプリケーション実行モジュール（アプリケーション実行手段）40は、ストレージ10、20におけるコンテンツにアクセスし、そのコンテンツに対する処理を行なうアプリケーションを動作させるものである。

【0020】オペレーティングシステム50は、アプリケーションの実行を制御するソフトウェアである。本実施形態のオペレーティングシステム50は、マルチプロセスに対応可能なものであり、アプリケーション実行モジュール40がアプリケーションを実行する際にプロセス毎に識別情報（プロセスID）を付与し、そのプロセスIDを用いてアプリケーションを呼び出したり、アプリケーションがファイルシステム11、21を呼び出すときにストレージ10、20に応じた適切なファイルシステム11、21のAPI（Application Programming Interface）を呼び出したりするものである。

【0021】なお、図1では、ストレージ10の著作物ファイルにアクセスして動作しているアプリケーションによる2つのプロセスに対し、それぞれ、プロセスIDとして#A0、#A1を付与し、ストレージ10の著作

物ファイルにアクセスせずに動作しているアプリケーションによるプロセスに対し、プロセスIDとして#A2を付与した例が示されている。これらのプロセス#A0～#A2は、同一のアプリケーションによって実行されるものであっても、それぞれ異なるアプリケーションによって実行されるものであってもよい。

【0022】また、アプリケーションは、汎用のパーソナルコンピュータ上で動作するもので、本発明のデータ管理システム専用のものであることは特に要求されない。例えば編集ソフトウェアやWebブラウザがこれにあたる。アプリケーション実行モジュール40でアプリケーションを実行する際には、各アプリケーションの動作は、オペレーティングシステム50によってプロセスとして管理される。

【0023】アクセス監視モジュール（アクセス監視手段）60は、アプリケーション実行モジュール40で動作中のアプリケーションについての固有情報と各アプリケーション（各プロセス）がアクセスしているコンテンツについての固有情報とを対応付けて管理テーブル（リスト）61に登録し、この管理テーブル61を用いて各アプリケーションのコンテンツへのアクセス状況を監視するものである。

【0024】このとき、本実施形態では、アプリケーションについての固有情報としては、オペレーティングシステム50からプロセス毎に付与されるプロセスIDが用いられ、コンテンツについての固有情報としては、コンテンツを含む著作物ファイルのファイル名、もしくは、その著作物ファイルを含む論理ドライブのドライブ名が用いられる（後述する機能(1)参照）。

【0025】また、アプリケーション実行モジュール40がアプリケーション（プロセス）の実行を終了した場合、アクセス監視モジュール60は、そのアプリケーションについての固有情報（プロセスID）とこれに対応するコンテンツについての固有情報（ファイル名）とを管理テーブル61から削除する。

【0026】つまり、アクセス監視モジュール60は、アプリケーションのファイルアクセスを監視し、ファイルアクセスを行なったアプリケーション（プロセス）毎にアクセスした著作物ファイルのファイル名の一覧（管理テーブル61）を作成し、少なくともアプリケーションが終了するまでそのファイル名を記憶しておき、特にオペレーティングシステム50がアプリケーションにプロセスIDを与える場合には、その一覧にアプリケーション（プロセス）の固有情報としてプロセスIDを登録して記憶しておく。

【0027】そして、本実施形態のアクセス監視モジュール60は、以下のような機能(1)～(5)を有していてもよい。

機能(1)：暗号化ファイルシステム11で管理されるストレージ10（論理ドライブ#S0）に蓄積された著作

10

20

30

40

50

物ファイル(コンテンツ)をアプリケーションが読み出す際に、コンテンツについての固有情報として、アプリケーションが読み出したコンテンツを含む著作物ファイルのファイル名を管理テーブル61に登録する機能。登録されるファイル名には、アプリケーションが読み出したコンテンツを蓄積する論理ドライブのドライブ名が含まれている。

【0028】機能(2):アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルのファイル名を、アプリケーションについての固有情報(プロセスID)に対応させて、管理テーブル61に登録する機能。このとき、新たに生成されたファイルのファイル名の一部もしくは全部を変更したものを管理テーブル61に登録してもよい。ここで用いられるファイル名は、そのファイルが蓄積される論理ドライブのドライブ名を含む文字列であり、そのドライブ名の部分を変更することにより、ファイルの蓄積先媒体(ストレージ10, 20)を変更したり、そのファイルをメモリファイルとして一次記憶手段(蓄積媒体; 図示省略)に一時的に記憶させたりすることができる。また、暗号化ファイルシステム11(ストレージ10)から読み出された著作物ファイルのファイル名を、新たに生成されたファイルのファイル名として登録・記憶してもよい。

【0029】機能(3):アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と、上記機能(1)により管理テーブル61に登録された論理ドライブのドライブ名(ファイル名に含まれるドライブ名)とを比較し、その比較結果が不一致である場合、管理テーブル61に登録されたドライブ名の論理ドライブに新たに生成されたファイルが蓄積されるように、そのファイル名を変更して管理テーブル61に登録する機能。即ち、新たに生成されたファイルの蓄積先論理ドライブと、コンテンツ(著作物ファイル)を蓄積している論理ドライブとが異なる場合、同じ論理ドライブ(同じストレージ10)に新たなファイルが生成されるようにファイル名を変更して管理テーブル61に登録する機能。この機能(3)により、新たに生成されたファイルを、元のコンテンツと同じ論理ドライブ(同じストレージ10)に生成・蓄積することができ、暗号化機能ありのストレージ10から読み出されたコンテンツに基づいて生成されたファイルは、暗号化ファイルシステム11により暗号化されてからストレージ10に書き込まれることになる。

【0030】機能(4):アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と、上記機能(1)により管理テーブル61に登録された論理ドライブのドライブ名(ファイル名に含まれるドライブ名)とを比較し、その比較結果が一致した場合、新たに生成されたファイルのファイル名の、管理テーブル61への登録を禁止す

る機能。つまり、新たに生成されたファイルの蓄積先論理ドライブと、コンテンツ(著作物ファイル)を蓄積している論理ドライブとが同じ場合、新たに生成されたファイルは、後述のフィルタモジュール70による暗号化処理を施さなくても、暗号化ファイルシステム11により暗号化されてからストレージ10に書き込まれることになる。従って、このような場合、本実施形態では、新たに生成されたファイルのファイル名の、管理テーブル61への登録を禁止してそのファイル名を登録・記憶しないようにすることにより、フィルタモジュール70が、無駄な暗号化処理を行なわないようにすることができる。

【0031】機能(5):アプリケーションによるコンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と、上記機能(1)により管理テーブル61に登録された論理ドライブのドライブ名(ファイル名に含まれるドライブ名)とを比較し、その比較結果が不一致である場合、後述するごとくフィルタモジュール70により新たに生成されたファイルを暗号化してから蓄積先論理ドライブ(ストレージ11)に蓄積させる機能。つまり、新たに生成されたファイルの蓄積先論理ドライブと、コンテンツ(著作物ファイル)を蓄積している論理ドライブとが異なる場合、フィルタモジュール70の動作を有効化する機能。このとき、上記機能(2)を用い、後述するフィルタモジュール70が、暗号化した新たに生成されたファイルを、蓄積先論理ドライブに代えて一次記憶手段にメモリファイルとして一時的に蓄積するように、そのファイル名の一部もしくは全部を変更して管理テーブル61に登録してもよい。

【0032】上述したアクセス監視モジュール60の機能を用いて、図1に示す管理テーブル61には、ストレージ10の著作物ファイルにアクセスして動作しているアプリケーションによる2つのプロセスの識別情報#A0, #A1が登録されている。そして、プロセス#A0については、このプロセス#A0によってアクセスされている著作物ファイルのファイル名#D0(論理ドライブ名#S0を含む)が登録されるとともに、このプロセス#A0により著作物ファイル#D0に基づいて生成・展開された2つの新たなファイルのファイル名\$file#F1, \$file#F2が登録されている。同様に、プロセス#A1については、このプロセス#A1によってアクセスされている著作物ファイルのファイル名#D1(論理ドライブ名#S0を含む)が登録されるとともに、このプロセス#A1により著作物ファイル#D1に基づいて生成・展開された2つの新たなファイルのファイル名\$file#F3, \$file#F4が登録されている。

【0033】なお、ファイル\$file#F1~\$file#F2は、後述するフィルタモジュール70により暗号化され、ファイルシステム21を通じて暗号化機能のないス

ストレージ 20 に蓄積されている。また、アクセス監視モジュール 60 の処理手順については、図 2 を参照しながら後述する。

【0034】フィルタモジュール（フィルタリング手段）70 は、アクセス監視モジュール 60 で作成した管理テーブル 61 を参照し、動作中のアプリケーション（プロセス）が、コンテンツを含むデータを、暗号化機能のないストレージ 20 において新たに生成されたファイルに書き込む際には、アプリケーションについての固有情報、即ちプロセス ID により生成された暗号鍵を用いてコンテンツを含むデータ（ファイル）を暗号化するものである。逆に、動作中のアプリケーション（プロセス）が、上述のごとく暗号化されたデータを、暗号化機能のないストレージ 20 のファイルから読み出す際には、フィルタモジュール 70 は、上述のごとく生成される暗号鍵を用いてデータ（コンテンツ）を復号化するのである。

【0035】なお、暗号化されたファイルをストレージ間で単に移動する際、フィルタモジュール 70 による暗号化処理／復号化処理は実行されない。また、フィルタモジュール 70 の処理手順については、図 3 を参照しながら後述する。さらに、ユーザがパスワードを入力することにより、フィルタモジュール 70 による暗号化処理／復号化処理を有効化／無効化して運用上の不都合を解決するため、フィルタモジュール 70 には、認証モジュール 71 および切替モジュール 72 がそなえられている。

【0036】認証モジュール（認証手段）71 は、ユーザの本人認証を行なうためのもので、ユーザによって入力されたパスワードと予め登録されている当該ユーザのパスワードとを比較し、これらが一致した場合にパスワードを入力したユーザが本人であることを認証するものである。切替モジュール（切替手段）72 は、認証モジュール 71 によってユーザの本人認証が行なわれた場合にのみフィルタモジュール 70 の動作の有効化／無効化を切り替えるものである。

【0037】上述したアプリケーション実行モジュール 40、アクセス監視モジュール 60、フィルタモジュール 70、認証モジュール 71 および切替モジュール 72 は、専用ソフトウェア（データ管理プログラム）によって実現される。このデータ管理プログラムは、例えばフレキシブルディスク、CD-ROM 等のコンピュータ読取可能な記録媒体に記録された形態で提供される。本実施形態においては、汎用のパーソナルコンピュータ（データ処理装置）を成す ROM（Read Only Memory；図示省略）等に予めデータ管理プログラムを格納しておき、このデータ管理プログラムを、やはり汎用のパーソナルコンピュータ（データ処理装置）を成す CPU（図示省略；コンピュータ）によって読み出し実行することで、上述したアプリケーション実行モジュール 40、アクセ

ス監視モジュール 60、フィルタモジュール 70、認証モジュール 71 および切替モジュール 72 としての機能が実現される。

【0038】なお、データ管理プログラムは、例えば磁気ディスク、光ディスク、光磁気ディスク等の記憶装置（記録媒体）に記録しておき、その記憶装置から通信経路を介してコンピュータに提供されてもよい。また、上述したストレージ 10、20 は、汎用のパーソナルコンピュータ（データ処理装置）を成すコンピュータに内蔵された RAM（Random Access Memory；図示省略）やハードディスクなどの記憶装置（あるいは外付けの記憶装置）によって実現される。

【0039】次に、図 2 および図 3 を参照しながら、上述のごとく構成された第 1 実施形態のデータ管理システムの動作について説明する。まず、図 2 に示すフローチャート（ステップ S11～S22）に従って、第 1 実施形態のデータ管理システムにおけるアクセス監視モジュール 60 の処理手順について説明する。

【0040】アクセス監視モジュール 60 は、アプリケーションの処理のために復号化された著作物データおよびその一部が、暗号化されずにストレージ 20 に保存されることを防止するため、暗号化すべきデータの一覧（管理テーブル 61）を作成する。

【0041】そのための動作について、図 2 に示すフローチャートに従って説明すると、アクセス監視モジュール 60 は、初期設定を行なった後（ステップ S11）、アプリケーション（プロセス）からオペレーティングシステム 50 に対する関数の呼出（Call）が行なわれたか否かを判定する（ステップ S12）。関数の呼出が行なわれた場合（ステップ S12 の YES ルート）、呼出（Call）対象の関数がリード関数であるか否かを判定する（ステップ S13）。

【0042】リード関数である場合（ステップ S13 の YES ルート）、リード対象のファイルの暗号属性を取得してから（ステップ S14）、そのファイルが、暗号化されている著作物データ（著作物ファイル）であるか否かを判定する（ステップ S15）。著作物データである場合（ステップ S15 の YES ルート）、管理テーブル 61 にアプリケーションの固有情報（オペレーティングシステム 50 によって付与されたプロセス ID）と、著作物データのファイル名（論理ドライブ名を含む）とを登録する（ステップ S16）。このとき、上述した機能 (i) が用いられる。この後、オペレーティングシステム 50 に対する関数の呼出（Call）を行ない（ステップ S17）、ステップ S12 に戻る。

【0043】呼出（Call）対象の関数がリード関数ではない場合（ステップ S13 の NO ルート）や、リード対象のファイルが、著作物データではなく、暗号化する必要のないものである場合（ステップ S15 の NO ルート）には、直ちにステップ S17 へ移行する。

【0044】一方、アプリケーション（プロセス）からオペレーティングシステム50に対する関数の呼出が行なわれなかった場合（ステップS12のNOルート）には、オペレーティングシステム50から登録対象アプリケーションへのオープン関数のリターンが行なわれ、且つ、ファイルのオープンに成功しているか否かを判定する（ステップS18）。

【0045】オープン関数のリターンが行なわれ、且つ、ファイルのオープンに成功している場合（ステップS18のYESルート）、そのファイルの保存先論理ドライブ（蓄積先論理ドライブ）のドライブ名を取得してから（ステップS19）、そのドライブ名が、管理テーブル61に登録されている著作物データ（著作物ファイル）の蓄積先論理ドライブのドライブ名と同じか否か、つまり、そのファイルの蓄積先論理ドライブと著作物データの蓄積先論理ドライブとが同一か否かを判定する（ステップS20）。

【0046】同一ではないと判定された場合（ステップS20のNOルート）、管理テーブル61において、登録対象アプリケーションの固有情報（オペレーティングシステム50によって付与されたプロセスID）に対応付けて、オープンされたファイルのファイル名を登録する（ステップS21）。このとき、上述した機能(2)や機能(5)が用いられる。この後、登録対象アプリケーションに対するオープン関数のリターンを行なった後（ステップS22）、ステップS12に戻る。

【0047】オープン関数のリターンが行なわれなかった場合やファイルのオープンに失敗している場合（ステップS18のNOルート）には、直ちにステップS22へ移行する。また、ファイルの蓄積先論理ドライブと著作物データの蓄積先論理ドライブとが同一であると判定された場合（ステップS20のYESルート）にも、後述する理由により、ステップS21による登録を行なうことなく、直ちにステップS22へ移行する。このとき、上述した機能(4)が用いられる。なお、ステップS21では、機能(2)に代えて、上述した機能(3)を用いてもよい。

【0048】ここで、アクセス監視モジュール60の動作をより具体的に説明する。まず、アクセス監視モジュール60は、アプリケーション（プロセス）のファイルアクセスを監視して、著作物データにアクセスしたアプリケーションに対して、アプリケーション固有の情報を取得する。例えば、オペレーティングシステム50のカーネルモジュールのラッパーモジュールによって、アプリケーションのファイルアクセスAPI呼出しを検出し、呼出し元のアプリケーションのプロセスIDを取得する。プロセスIDの他にもアプリケーション名や検出時刻などを合わせて取得してもよい。アクセス監視モジュール60は、さらに著作物データを含むファイルのファイル名を取得する。そして、取得されたアプリケーシ

ョン固有の情報や著作物データのファイル名は対応付けられて管理テーブル51に登録される（ステップS16）。ファイル名は、前述した通り、蓄積されている論理ドライブ名を含む文字列である。

【0049】ステップS15においてリード対象のファイルが著作物データであるか否かを判定する際、そのファイルが保存されている論理ドライブに利用されているファイルシステムが暗号化ファイルシステムであることが予め認識されていれば、そのことだけでリード対象のファイルが著作物データとみなしてもよく、暗号化ファイルシステムがファイルやフォルダに対して暗号属性を設定するものである場合には、この暗号属性を利用して著作物データの判定を行なう。

【0050】また、アクセス監視モジュール60は、ステップS15において上述のように著作物データであるか否かを判定する際、ファイルシステムから得られる情報だけでなく、Webブラウザやストリーミング映像再生アプリケーションなどで行なわれるようにサーバ接続時の認証手続きをフックしてもよい。ストリーミング映像再生アプリケーションは再生処理のためにストレージに中間ファイルを生成することがある。特に、ストリーミングにおける著作権保護では、ダウンロードと異なり、ストレージに蓄積しないことが前提となっているので、上述のようにストリーミング映像サーバとの認証手続きをフックすることによって、この中間ファイルに対しても後述の暗号化処理を適用することが可能となる。

【0051】一方、アクセス監視モジュール60は、登録対象アプリケーションが新たにファイルを生成する際にそのファイル名を取得し、暗号化対象ファイルとして管理テーブル61に登録する。暗号化対象ファイルが登録対象アプリケーションによってアクセスされた著作物データと同じ論理ドライブに蓄積される場合（ステップS20のYESルート）には、次の考え方から、管理テーブル61に対する登録を行なう必要がない。

【0052】一つ目の考え方は、著作物データが蓄積されている論理ドライブ（ストレージ10）であれば、暗号化対象ファイルは、自動的に、暗号化ファイルシステム11によって暗号化されて、その論理ドライブに蓄積されるためである。二つ目の考え方は、著作物データが蓄積されている論理ドライブ（ストレージ10）であれば、データが外部へ流出することがないためである。

【0053】逆に、これらの考え方から、ステップS21において上述した機能(3)を用いて、暗号化対象ファイルのファイル名の一部を変更することにより、著作物データが蓄積されている論理ドライブに暗号化対象ファイルが蓄積されるようにすることも有効である。例えば、アプリケーションからの暗号化対象ファイルへのアクセスをフックし、ファイル名の論理ドライブ名をあらわす文字列を、著作物データが蓄積されている論理ドライブのドライブ名に置き換えるような変更を行なう。こ

れは、著作物データと異なる論理ドライブへのファイルの書き込みを禁止する場合に有効である。

【0054】アクセス監視モジュール60は、アプリケーション実行モジュール40で登録対象アプリケーションが動作を終了する際に、管理テーブル61からそのアプリケーションに関するデータを全て消去する。つまり、アプリケーション固有の情報、著作物データのファイル名、暗号化対象ファイル名などが管理テーブル61から除かれる。

【0055】ついで、図3に示すフローチャート(ステップS31~S45)に従って、第1実施形態のデータ管理システムにおけるフィルタモジュール70の処理手順について説明する。フィルタモジュール70は、アプリケーションからのファイルアクセスに応じて、管理テーブル61を参照して暗号化/復号化を行なう。

【0056】その動作について、図3に示すフローチャートに従って説明すると、フィルタモジュール70は、初期設定を行なった後(ステップS31)、ファイルシステム関数の呼出(Call)が行なわれたか、もしくは、ファイルシステム関数からの復帰(Return)が行なわれたかを判定する(ステップS32)。ファイルシステム関数の呼出が行なわれた場合(ステップS32のYESルート)、ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール72で有効化されているかを判定する(ステップS33)。

【0057】ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール72により有効化されている場合(ステップS33のYESルート)、そのファイルに対するアクセスがライトアクセスであるかを判定する(ステップS34)。ファイルへのアクセスがライトアクセスである場合(ステップS34のYESルート)、管理テーブル61を参照してアプリケーションの固有情報(プロセスID)を取得し、そのプロセスIDから暗号鍵を生成し(ステップS35)、その暗号鍵を用いてライト対象のデータを暗号化する(ステップS36)。この後、処理をファイルシステムに渡し(ファイルシステム関数CALL;ステップS37)、ステップS32に戻る。

【0058】ファイルへのアクセスがライトアクセスではない場合(ステップS34のNOルート)、そのアクセスがリードアクセスであるかを判定する(ステップS38)。ファイルへのアクセスがリードアクセスである場合(ステップS38のYESルート)、管理テーブル61を参照してファイル名変更が必要であるかを判定する(ステップS39)。

【0059】ファイル名変更が必要である場合(ステップS39のYESルート)、そのファイル名を変更する(ステップS40)。この後、処理をファイルシステムに渡し(ステップS37)、ステップS32に戻る。ファイルが暗号化対象でない場合や暗号化機能が切替モジ

ジュール72により有効化されていない場合(ステップS33のNOルート)、あるいは、暗号化対象ファイルへのアクセスがリードアクセスでない場合(ステップS38のNOルート)、あるいは、そのファイルへのファイル名変更が必要でない場合(ステップS39のNOルート)、直ちにステップS37へ移行する。

【0060】一方、ファイルシステム関数からの復帰(Return)の場合(ステップS32のNOルート)、ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール72で有効化されているかを判定する(ステップS41)。ファイルが暗号化対象であり、且つ、暗号化機能が切替モジュール72により有効化されている場合(ステップS41のYESルート)、そのファイルに対するアクセスがリードアクセスであるかを判定する(ステップS42)。

【0061】ファイルへのアクセスがリードアクセスである場合(ステップS42のYESルート)、管理テーブル61を参照してアプリケーションの固有情報(プロセスID)を取得し、そのプロセスIDから暗号鍵を生成し(ステップS43)、その暗号鍵を用いてリード対象のデータを復号化する(ステップS44)。この後、処理をファイルシステム関数の呼出元に渡し(RETURN;ステップS45)、ステップS32に戻る。

【0062】ファイルが暗号化対象でない場合や暗号化機能が切替モジュール72により有効化されていない場合(ステップS41のNOルート)、あるいは、暗号化対象ファイルへのアクセスがリードアクセスでない場合(ステップS42のNOルート)、直ちにステップS45へ移行する。

【0063】ここで、フィルタモジュール70の動作をより具体的に説明する。上述した通り、暗号鍵は、管理テーブル61に登録されているアプリケーション固有の情報をを用いて生成される。例えば、前述したようにオペレーティングシステム50によって与えられたプロセスIDを利用することが考えられる。

【0064】プロセスIDを暗号鍵として利用して暗号化されたファイルは、他の登録対象アプリケーションからアクセスされたとしても、異なる暗号鍵が使用されることになるので、復号化されない。さらに、同じアプリケーションで同様の手順で暗号化ファイルにアクセスしようとしても、やはりプロセスIDが異なるので、暗号鍵を生成してもその暗号化ファイルを復号化することはできない。

【0065】なお、偶然に同じプロセスIDを持つアプリケーションが存在しても、異なる登録対象アプリケーションによる暗号化ファイルの復号化が行なわれることを防ぐためには、プロセスIDとともに時刻情報なども暗号鍵生成に利用することが有効である。例えば、登録対象アプリケーションによる著作物データへのファイルアクセスをアクセス監視モジュール60が検出した時

刻などを用いる。また、登録対象アプリケーションによるファイル生成をアクセス監視モジュール60が検出した時刻を用いてもよい。時刻情報を加味することにより同一暗号鍵生成を防ぐことができる理由は、オペレーティングシステム50が同一のシステム上で同時刻に同じプロセスIDを与え得ないからである。

【0066】暗号鍵は、フィルタモジュール70内のみ保持され、通信路で伝送されたりストレージ10、20に保存されることはない。暗号鍵の盗難の可能性は低い。しかし、オペレーティングシステムによって、プロセスIDを比較的容易に取得することが可能であるので、より堅牢性を高めるために、上述のアプリケーション固有の情報から擬似乱数を演算したものを作業鍵として用いてもよい。

【0067】データに対する暗号化アルゴリズムについては、ファイルが、通常、バイト列として扱われるので、ブロック暗号方式が適している。フィルタモジュール70は、オペレーティングシステム50からのファイルアクセスをフックして暗号化あるいは復号化を行なう(ステップS34またはS44)。ライトアクセスの場合は、オペレーティングシステム50を経由して受け取ったデータ(ファイル)を、上述のように暗号化した後、ファイルシステム21に渡す。リードアクセスの場合は、ファイルシステム21から受け取った暗号化データを復号化してオペレーティングシステム50に渡す。

【0068】なお、暗号化対象ファイルが、管理テーブル61に登録されている著作物データが蓄積されている論理ドライブ(または蓄積媒体)と同じ論理ドライブ(または蓄積媒体)に生成される場合、ある特定の暗号化ファイルシステム、あるいはファイルやフォルダ毎に暗号属性を設定可能な暗号化ファイルシステムに対しては、暗号化対象ファイルに対してフィルタモジュール70で暗号化/復号化を行なう必要がない。

【0069】また、著作者自身や、著作者の許諾を得た者、例えば著作物を編集するなど二次著作物を生成する者に対しては、フィルタモジュール70の暗号化/復号化処理を無効化する必要がある。そこで、本実施形態では、所定のパスワードによりフィルタモジュール70の暗号化/復号化処理を無効化できるようになっている。

【0070】つまり、ユーザが、フィルタモジュール70の暗号化/復号化処理を無効化もしくは有効化する際には、認証モジュール71に対してパスワードを入力する。この認証モジュール71においては、ユーザによって入力されたパスワードと予め登録されている当該ユーザのパスワードとが比較され、これらが一致した場合にパスワードを入力したユーザが本人であると認証される。そして、認証モジュール71によってユーザの本人認証が行なわれた場合にのみ、切替モジュール72により、フィルタモジュール70の動作は有効状態から無効状態に切り替えられる。

【0071】このように、本発明の第1実施形態としてのデータ管理システムによれば、暗号機能ありのストレージ10、20に蓄積されたコンテンツがアプリケーションによってアクセスされると、そのアクセス状況がアクセス監視モジュール60によってアプリケーション

(プロセス)毎に管理され、アプリケーションによって読み出されて利用されているコンテンツは、そのアプリケーションについての固有情報であるプロセスIDを用いフィルタモジュール70によって暗号化/復号化される。

【0072】そして、暗号化ファイルシステム11によってストレージ10に蓄積された、暗号化された著作物データをアプリケーションが利用する場合、その暗号化データを一旦復号化する必要がある。このアプリケーションが新たに生成したファイルには、復号化された著作物データが含まれる可能性が高い。そこで、本実施形態では、少なくとも暗号化された著作物データをアプリケーションがアクセスする際、アクセス監視モジュール60が管理テーブル61にアプリケーションの固有情報を登録し、さらにアプリケーションが新たに生成しようとするファイルのファイル名も登録しておくことで、アプリケーションが、読み出し元の暗号機能のあるストレージ10ではない、暗号機能のないストレージ20に書き込むファイルに対して、フィルタモジュール70がデータを暗号化することが可能となる。

【0073】これにより、暗号化機能なしのストレージ20と暗号化機能ありのストレージ10とを混在させて使用する状況下において、アプリケーションが、暗号機能ありのストレージ10に蓄積された暗号化コンテンツ(著作物データ)を読み出し、そのコンテンツを暗号化機能なしのストレージ20に一時的に新しいファイルとして格納しながら利用したとしても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護することができ、データ管理システムの性能向上に寄与するところが大きい。

【0074】つまり、ディジタル化された著作物データ(ディジタルコンテンツ)が暗号化された上で暗号機能なしのストレージ20に蓄積されるので、ユーザが誤って著作物データを第三者に渡すなどによって著作権が侵害されるのを防ぐことができる。また、悪意のある者が故意にストレージ20のみを取り外し、蓄積されたデータの内容を見ようと試みようとしても、基本的にデータが暗号化されているので、その者は意味のあるデータを得ることができないので、著作権が侵害されるのを防ぐことができる。

【0075】アプリケーションが読み出し元と同じストレージ10、20に新たなファイルを生成してそのファイルにコンテンツを格納する場合、そのコンテンツは、ストレージ10、20毎のファイルシステムに従って書き込まれる。つまり、アプリケーションが元々暗号化さ

れていないファイルのコンテンツにアクセスしている間は、暗号化を施すことなくコンテンツが書き込まれる。一方、アプリケーションが、暗号化ファイルシステム 11 で管理される論理ドライブから暗号化ファイルを読み出し、読み出し元以外に新たなファイルを生成してそのファイルにコンテンツ（著作物データ）を格納する場合、そのコンテンツ（ファイル）は、アプリケーションの固有情報（プロセス ID）で暗号化されるので、アプリケーションが処理を終了するまでは、そのファイルを生成したアプリケーションのみがそのコンテンツ（ファイル）を復号化して利用することができる。

【0076】このとき、アプリケーションについての固有情報として、オペレーティングシステム 50 によって与えられるプロセス ID のような動的な情報を用い、その情報でコンテンツの暗号化を行なうことにより、同じアプリケーションであっても起動時期が異なると復号化することができず、暗号機能なしのストレージ 20 上のファイルを通して復号化されたデータが容易に交換されなくなるので、著作権の侵害をより確実に防ぐことができる。

【0077】また、ユーザの本人認証が行なわれた場合にのみフィルタモジュール 70 の動作の有効化／無効化を切り替えることにより、著作者自身や著作者の許諾を得た者（例えば著作物を編集するなど二次著作物を生成する者）を登録しておけば、著作者自身や著作者の許諾を得た者は、フィルタモジュール 70 の動作（暗号化／復号化処理）を無効化することができ、作業を不当に制限されず、著作権の行使の著しい制限に伴う著作権侵害の発生を防止することができる。

【0078】さらに、ストレージ 10（論理ドライブ # S0）が、コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有しファイル毎またはフォルダ毎に暗号化を行なった上でコンテンツ（著作物ファイル）をストレージ 10 に蓄積させる暗号化ファイルシステム 11、もしくは、そのファイルシステムの全体を暗号化した上でコンテンツ（著作物ファイル）をストレージ 10 に蓄積させる暗号化ファイルシステム 11 によって管理され、デジタル化された著作物データが暗号化された上でストレージ 10 に蓄積されているので、ユーザが誤って著作物データを第三者に渡すなどによって著作権が侵害されるのを防ぐことができる。また、悪意のある者が故意にストレージ 10 のみを取り外し、蓄積されたデータの内容を見ようと試みようとしても、基本的にデータが暗号化されているので、その者は意味のあるデータを得ることができないので、著作権が侵害されるのを防ぐことができる。

【0079】また、アクセス監視モジュール 60 の機能 (5) を用いることにより、フィルタモジュール 70 が、暗号化した新たに生成されたファイルを、蓄積先論理ドライブに代えて一次記憶手段にメモリファイルとして一

時的に蓄積するように、そのファイル名の一部もしくは全部が変更されて管理テーブル 61 に登録される。これにより、新たに生成されたファイルは、フィルタモジュール 70 によって暗号化された上で一次記憶手段に記憶されるので、一旦、電源が切られると、一次記憶手段に蓄積された暗号化ファイルは、消去され、一次記憶手段に保持され続けることがないので、より確実に著作権が侵害されるのを防ぐことができる。

【0080】〔1-1〕第 1 実施形態の変形例の説明

図 4 は第 1 実施形態のデータ管理システムの変形例の構成を示すブロック図であり、この図 4 において、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているのので、その説明は省略する。

【0081】図 1 に示す第 1 実施形態のデータ管理システムでは、2 つのストレージ 10 および 20 をそなえ、各ストレージ 10、20 に一つの論理ドライブ # S0、# S1 が構築されている場合について説明したが、図 4 に示すごとく、2 つのストレージ 10、20 に代えて一つのストレージ（蓄積媒体）80 をそなえ、このストレージ 80 を複数（図 4 では 2 つ）のパーティションに分け、これらのパーティションをそれぞれ論理ドライブ # P0、# P1 として用いてもよい。

【0082】ここで、論理ドライブ # P0 は、暗号化ファイルシステム 11 によって管理され暗号化機能ありの蓄積媒体（図 1 の論理ドライブ # S0 に対応）として機能するとともに、ファイルシステム 21 によって管理され論理ドライブ # P1 は、暗号化機能なしの蓄積媒体（図 1 の論理ドライブ # S1 に対応）として機能する。この場合も、本発明は、上述した第 1 実施形態と同様に適用され、上述した第 1 実施形態と同様の作用効果を得ることができる。

【0083】〔2〕第 2 実施形態の説明

図 5 は本発明の第 2 実施形態としてのデータ管理システムの構成を示すブロック図であり、この図 5 に示すように、第 2 実施形態のデータ管理システムも第 1 実施形態のものと同様に構成されているが、第 2 実施形態のデータ管理システムは、汎用のパーソナルコンピュータ等のデータ処理装置 100 と、このデータ処理装置 100 に例えば LAN (Local Area Network) 等の有線ネットワークもしくは無線ネットワークを介して接続されたデータ記録再生装置 200 とから構成されている。なお、図 5 において、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているのので、その説明は省略する。

【0084】データ処理装置 100 は、第 1 実施形態で上述したストレージ 10、暗号化ファイルシステム 11、ストレージ 20、ファイルシステム 21、上位ファイルシステム 30、アプリケーション実行モジュール 40、オペレーティングシステム 50、アクセス監視モジュール 60、フィルタモジュール 70、認証モジュール 71 および切替モジュール 72 をそなえて構成されると

ともに、さらにネットワークファイルシステム 101 をそなえている。

【0085】ネットワークファイルシステム 101 は、外部の有線ネットワークもしくは無線ネットワークとのインタフェース機能を果たし、且つ、データ記録再生装置 200 における暗号機能なしのストレージ（蓄積媒体）を管理するものである。また、データ記録再生装置 200 は、フィルタモジュール 70 によって暗号化されたコンテンツ（著作物ファイル／著作物データ）を蓄積する第 2 蓄積装置として機能し、暗号機能なしのストレージ 20 と同様の機能を果たすものである。このデータ記録再生装置 200 におけるストレージには、データ処理装置 100 側からは、ネットワークファイルシステム 101 を介してアクセスされる。ただし、データ記録再生装置 200 におけるストレージから読み出されたデータは、ネットワークを介してデータ処理装置 100 で受け取られるまで、暗号化されたままである。なお、処理手順については第 1 実施形態と同様であるので、その説明は省略する。

【0086】このように、本発明の第 2 実施形態としてのデータ管理システムによれば、第 1 実施形態と同様の作用効果が得られるほか、ユーザが誤ってネットワーク経由でデータ複製を行なったとしても、著作権を侵害することがない。

【0087】〔3〕第 3 実施形態の説明

図 6 は本発明の第 3 実施形態としてのデータ管理システムの構成を示すブロック図、図 7 は第 3 実施形態のデータ管理システムにおける排他制御手法について説明するための図である。図 6 に示すように、第 3 実施形態のデータ管理システムも第 1 実施形態のものと同様に構成されているが、第 3 実施形態のデータ管理システムは、汎用のパーソナルコンピュータ等のデータ処理装置 100 と、このデータ処理装置 100 に外付けされたハードディスクレコーダ等のデータ記録再生装置 300 とから構成されている。なお、図 6 や図 7 において、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その説明は省略する。

【0088】第 3 実施形態のデータ処理装置 100 には、第 1 実施形態で上述した暗号化ファイルシステム 11、ストレージ 20、ファイルシステム 21、上位ファイルシステム 30、アプリケーション実行モジュール 40、オペレーティングシステム 50、アクセス監視モジュール 60、フィルタモジュール 70、認証モジュール 71 および切替モジュール 72 がそなえられており、ストレージ 10 は、外付けのデータ記録再生装置 300 に含まれている。つまり、第 3 実施形態では、データ記録再生装置 300 が、暗号化ファイルシステム 11、301 で管理される論理ドライブを含む第 1 蓄積装置として機能する。

【0089】なお、データ記録再生装置 300 には、ス

トレージ 10 を管理する暗号化ファイルシステム 301 もそなえられている。そして、図 7 に示すごとく、第 3 実施形態のデータ記録再生装置 300 においてもアプリケーションが動作し、このアプリケーションが、暗号化ファイルシステムストレージ 10 に蓄積された著作物ファイルに対するファイルアクセスを行なうようになって

【0090】データ処理装置 100 とデータ記録再生装置 300 とは、USB (Universal Serial Bus)、SCSI (Small Computer System Interface)、IEEE (Institute of Electrical and Electronics Engineers) 1394 などの外部インタフェースを介して接続される。そして、データ処理装置 100 は、データ記録再生装置 300 側のストレージ 10 を排他制御しながら、このストレージ 10 にアクセスする。

【0091】上述した第 2 実施形態では、データ処理装置 100 がネットワークファイルシステム 101 を介してデータ記録再生装置 200 のストレージにアクセスするので、データ記録再生装置 200 がファイルアクセスのサービスを提供するのに対して、第 3 実施形態では、データ処理装置 100 側の暗号化ファイルシステム 11 が、直接、データ記録再生装置 300 のストレージ 10 にアクセスする点で異なっている。なお、処理手順については第 1 実施形態と同様であるので、その説明は省略する。

【0092】第 3 実施形態では、データ記録再生装置 300 におけるストレージ 10 に対しては、このデータ記録再生装置 300 内のアプリケーションとデータ処理装置 100 側のアプリケーションとの両方からアクセスが行なわれることになるため、排他制御を行なう必要がある。ここで、図 7 を参照しながら、第 3 実施形態のデータ管理システムにおける排他制御手法について説明する。なお、図 7 においては、第 3 実施形態のデータ管理システムの要部のみが図示されている。

【0093】図 7 に示すように、データ処理装置 100 側には制御モジュール 102 がそなえられるとともに、データ記録再生装置 300 側には制御モジュール 302 がそなえられており、これらの制御モジュール 102 と 302 とが上述した外部インタフェースを介して接続され、排他制御を行なうための制御情報（排他制御信号）が、データ処理装置 100 とデータ記録再生装置 300 との間でやり取りされるようになっている。

【0094】また、図 7 に示すように、データ処理装置 100 とデータ記録再生装置 300 との間では、制御情報をやり取りするための系統以外に、上述した外部インタフェースを介し、ストレージアクセスについての情報（暗号文リード／暗号文ライト）をやり取りするための系統もそなえられている。このとき、ストレージアクセスのための全ての権利を排他制御しても良く、ライトアクセスのみの権利を排他制御しても良い。

【0095】前者の排他制御手法では、データ処理装置100とデータ記録再生装置300とのうちのいずれか一方がストレージ10にアクセスしている間は、他方からのアクセスが禁止される。後者の排他制御手法では、データ処理装置100とデータ記録再生装置300とのうちのいずれか一方がライトアクセスしている間は、他方はリードアクセスのみが許可されライトアクセスは待たされる。リードアクセスを行なう権利は双方が有している。ただし、いずれもアクセス権を渡す場合には、暗号化ファイルシステム11、301などが持つキャッシュの内容を全てフラッシュしてストレージ10に書き込まなければならない。また、アクセス権を受け取った後については、少なくとも書き込み前に暗号化ファイルシステム11、301の管理情報を再読み込みしなければならない。

【0096】このように、本発明の第3実施形態としてのデータ管理システムによれば、第1や第2実施形態と同様の作用効果が得られる。

〔4〕その他

なお、本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。例えば、本実施形態の認証モジュール71では、パスワードによる本人認証を行なっているが、本発明はこれに限定されるものではなく、指紋、声紋、虹彩、掌形等のバイオメトリクス情報を用いて本人認証を行なってもよい。

【0097】〔5〕付記

（付記1）コンテンツを蓄積する蓄積媒体と、該蓄積媒体における該コンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴とする、データ管理システム。

【0098】（付記2）該アプリケーションの実行を制御するソフトウェアとしてのオペレーティングシステムをさらにそなえ、該アクセス監視手段が、該アプリケーションについての固有情報として、該アプリケーション実行手段が該アプリケーションを実行する際に該オペレーティングシステムから与えられるプロセス毎の識別情報を用いることを特徴とする、付記1記載のデータ管

理システム。

【0099】（付記3）該アクセス監視手段が、該アプリケーションについての固有情報と該コンテンツについての固有情報とを対応付けて管理テーブルに登録し、該管理テーブルを用いて該アクセス状況を監視することを特徴とする、付記1または付記2に記載のデータ管理システム。

（付記4）該アプリケーション実行手段が該アプリケーションの実行を終了した場合、該アクセス監視手段が、該アプリケーションについての固有情報とこれに対応する該コンテンツについての固有情報とを該管理テーブルから削除することを特徴とする、付記3記載のデータ管理システム。

【0100】（付記5）該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、該ファイルシステムのうちの少なくとも一つが、該コンテンツを含むファイル毎またはフォルダ毎に暗号属性を有し該ファイル毎または該フォルダ毎に暗号化を行なった上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、付記3または付記4に記載のデータ管理システム。

【0101】（付記6）該蓄積媒体において、少なくとも一つの論理ドライブが構築されるとともに該論理ドライブに該コンテンツが保存され、該論理ドライブを管理するファイルシステムが該論理ドライブ毎に構築され、該ファイルシステムの全体の暗号化した上で該コンテンツを該蓄積媒体に蓄積させる暗号化ファイルシステムであることを特徴とする、付記3または付記4に記載のデータ管理システム。

【0102】（付記7）該暗号化ファイルシステムで管理される該論理ドライブに蓄積された該コンテンツを該アプリケーションが読み出す際に、該アクセス監視手段が、該コンテンツについての固有情報として、該アプリケーションが読み出した該コンテンツを含むファイルのファイル名を該管理テーブルに登録することを特徴とする、付記5または付記6に記載のデータ管理システム。

【0103】（付記8）該暗号化ファイルシステムで管理される該論理ドライブに蓄積された該コンテンツを該アプリケーションが読み出す際に、該アクセス監視手段が、該コンテンツについての固有情報として、該アプリケーションが読み出した該コンテンツを含む論理ドライブのドライブ名を該管理テーブルに登録することを特徴とする、付記5または付記6に記載のデータ管理システム。

【0104】（付記9）該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴っ

て新たに生成されたファイルのファイル名を、該アプリケーションについての固有情報に対応させて、該管理テーブルに登録することを特徴とする、付記 5～付記 8 のいずれか一つに記載のデータ管理システム。

(付記 10) 該アクセス監視手段が、該新たに生成されたファイルのファイル名の一部もしくは全部を変更したものを該管理テーブルに登録することを特徴とする、付記 9 記載のデータ管理システム。

【0105】(付記 11) 該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と該管理テーブルに登録された該論理ドライブのドライブ名とを比較し、その比較結果が不一致である場合、該管理テーブルに登録された該ドライブ名の論理ドライブに該新たに生成されたファイルが蓄積されるように該ファイル名を変更して該管理テーブルに登録することを特徴とする、付記 8 記載のデータ管理システム。

【0106】(付記 12) 該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と該管理テーブルに登録された該論理ドライブのドライブ名とを比較し、その上記比較結果が一致した場合、該アクセス監視手段が、該新たに生成されたファイルのファイル名の、該管理テーブルへの登録を禁止することを特徴とする、付記 8 記載のデータ管理システム。

【0107】(付記 13) 該アクセス監視手段が、該アプリケーションによる該コンテンツに対する処理に伴って新たに生成されたファイルの蓄積先論理ドライブのドライブ名と該管理テーブルに登録された該論理ドライブのドライブ名とを比較し、その比較結果が不一致である場合、該フィルタリング手段の動作が有効化されることを特徴とする、付記 8 記載のデータ管理システム。

【0108】(付記 14) 該蓄積媒体が、電源断に伴って蓄積データを消去される一次記憶手段を含み、該フィルタリング手段が、暗号化した該新たに生成されたファイルを、該蓄積先論理ドライブに代えて該一次記憶手段に蓄積することを特徴とする、付記 13 記載のデータ管理システム。

【0109】(付記 15) 該蓄積媒体が、該暗号化ファイルシステムで管理される該論理ドライブを含む第 1 蓄積装置と、該フィルタリング手段によって暗号化された該コンテンツを蓄積する第 2 蓄積装置とを含んで構成されていることを特徴とする、付記 5～付記 14 のいずれか一つに記載のデータ管理システム。

【0110】(付記 16) 該アプリケーション実行手段、該アクセス監視手段、該フィルタリング手段および該第 1 蓄積装置が、一つのデータ処理装置内にそなえられるとともに、該第 2 蓄積装置が、ネットワークを介し

て該データ処理装置に接続されていることを特徴とする、付記 15 記載のデータ管理システム。

【0111】(付記 17) ユーザの本人認証を行なうための認証手段と、該認証手段によって該ユーザの本人認証が行なわれた場合にのみ該フィルタリング手段の動作の有効化/無効化を切り替える切替手段とをさらにそなえたことを特徴とする、付記 1～付記 16 のいずれか一つに記載のデータ管理システム。

【0112】(付記 18) 該アプリケーション実行手段、該アクセス監視手段、該フィルタリング手段および該第 2 蓄積装置が、一つのデータ処理装置内にそなえられるとともに、該第 1 蓄積装置が、該データ処理装置に外付けされるデータ記録再生装置に含まれていることを特徴とする、付記 16 記載のデータ管理システム。

【0113】(付記 19) 蓄積媒体に蓄積されたコンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションを動作させるアプリケーション実行手段と、該アプリケーション実行手段で動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段と、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段とをそなえて構成されたことを特徴とする、データ処理装置。

【0114】(付記 20) 蓄積媒体に蓄積されたコンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションが動作している際に、該コンテンツの著作権を保護する機能をコンピュータによって実現させるためのデータ管理プログラムであって、動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段、および、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段として、コンピュータを機能させることを特徴とする、データ管理プログラム。

【0115】(付記 21) 蓄積媒体に蓄積されたコンテンツにアクセスし該コンテンツに対する処理を行なうアプリケーションが動作している際に、該コンテンツの著作権を保護する機能をコンピュータによって実現させ

るためのデータ管理プログラムを記録したコンピュータ読取可能な記録媒体であって、該データ管理プログラムが、動作中の該アプリケーションについての固有情報と該アプリケーションがアクセスしている該コンテンツについての固有情報とを対応付けて、該アプリケーションの該コンテンツへのアクセス状況を監視するアクセス監視手段、および、動作中の該アプリケーションが該コンテンツを該蓄積媒体に書き込む際には該アプリケーションについての固有情報を用いて該コンテンツを暗号化する一方、動作中の該アプリケーションが該コンテンツを該蓄積媒体から読み出す際には該アプリケーションについての固有情報を用いて該コンテンツを復号化するフィルタリング手段として、該コンピュータを機能させることを特徴とする、データ管理プログラムを記録したコンピュータ読取可能な記録媒体。

【0116】

【発明の効果】以上詳述したように、本発明（請求項1～5）によれば、蓄積媒体に蓄積されたコンテンツがアプリケーションによってアクセスされると、そのアクセス状況がアプリケーション毎に管理され、アプリケーションによって読み出されて利用されているコンテンツは、そのアプリケーションについての固有情報を用いて暗号化／復号化される。

【0117】これにより、暗号化機能なしの蓄積媒体と暗号化機能ありの蓄積媒体とを混在させて使用する状況下において、アプリケーションが、暗号機能ありの蓄積媒体に蓄積された暗号化コンテンツを読み出し、そのコンテンツを暗号化機能なしの蓄積媒体に一時的に格納しながら利用したとしても、著作権の行使を不当に制限することなく、暗号化が解除されたコンテンツの著作権を確実に保護することができ、データ管理システムの性能向上に寄与するところ大きい。

【0118】つまり、デジタル化された著作物データ（デジタルコンテンツ）が暗号化された上で蓄積されるので、ユーザが誤って著作物データを第三者に渡すなどによって著作権が侵害されるのを防ぐことができる。また、悪意のある者が故意に蓄積媒体のみを取り外し、蓄積されたデータの内容を見ようと試みようとしても、基本的にデータが暗号化されているので、その者は意味のあるデータを得ることができないので、著作権が侵害されるのを防ぐことができる。

【0119】このとき、アプリケーションについての固有情報として、オペレーティングシステムによって与えられるプロセス毎の識別情報（プロセスID）のような動的な情報を用い、その識別情報でコンテンツの暗号化を行なうことにより、同じアプリケーションであっても起動時期が異なると復号化することができず、蓄積媒体上のファイルを通して復号化されたデータが容易に交換されなくなるので、著作権の侵害をより確実に防ぐことができる。

【0120】また、ユーザの本人認証が行なわれた場合にのみフィルタリング手段の動作の有効化／無効化を切り替えるように構成することにより、著作者自身や著作者の許諾を得た者（例えば著作物を編集するなど二次著作物を生成する者）を登録しておけば、著作者自身や著作者の許諾を得た者は、フィルタリング手段の動作を無効化することができ、作業を不当に制限されず、著作権の行使の著しい制限に伴う著作権侵害の発生を防止することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態としてのデータ管理システムの構成を示すブロック図である。

【図2】第1実施形態のデータ管理システムにおけるアクセス監視モジュールの処理手順を説明するためのフローチャートである。

【図3】第1実施形態のデータ管理システムにおけるフィルタモジュールの処理手順を説明するためのフローチャートである。

【図4】第1実施形態のデータ管理システムの変形例の構成を示すブロック図である。

【図5】本発明の第2実施形態としてのデータ管理システムの構成を示すブロック図である。

【図6】本発明の第3実施形態としてのデータ管理システムの構成を示すブロック図である。

【図7】第3実施形態のデータ管理システムにおける排他制御手法について説明するための図である。

【符号の説明】

10 ストレージ（暗号化機能ありの蓄積媒体、第1蓄積装置）

11 暗号化ファイルシステム

20 ストレージ（暗号化機能なしの蓄積媒体、第2蓄積装置）

21 ファイルシステム（FAT）

30 上位ファイルシステム

40 アプリケーション実行モジュール（アプリケーション実行手段）

50 オペレーティングシステム

60 アクセス監視モジュール（アクセス監視手段）

61 管理テーブル（リスト）

70 フィルタモジュール（フィルタリング手段）

71 認証モジュール（認証手段）

72 切替モジュール（切替手段）

80 ストレージ（蓄積媒体）

100 データ処理装置

101 ネットワークファイルシステム

102 制御モジュール

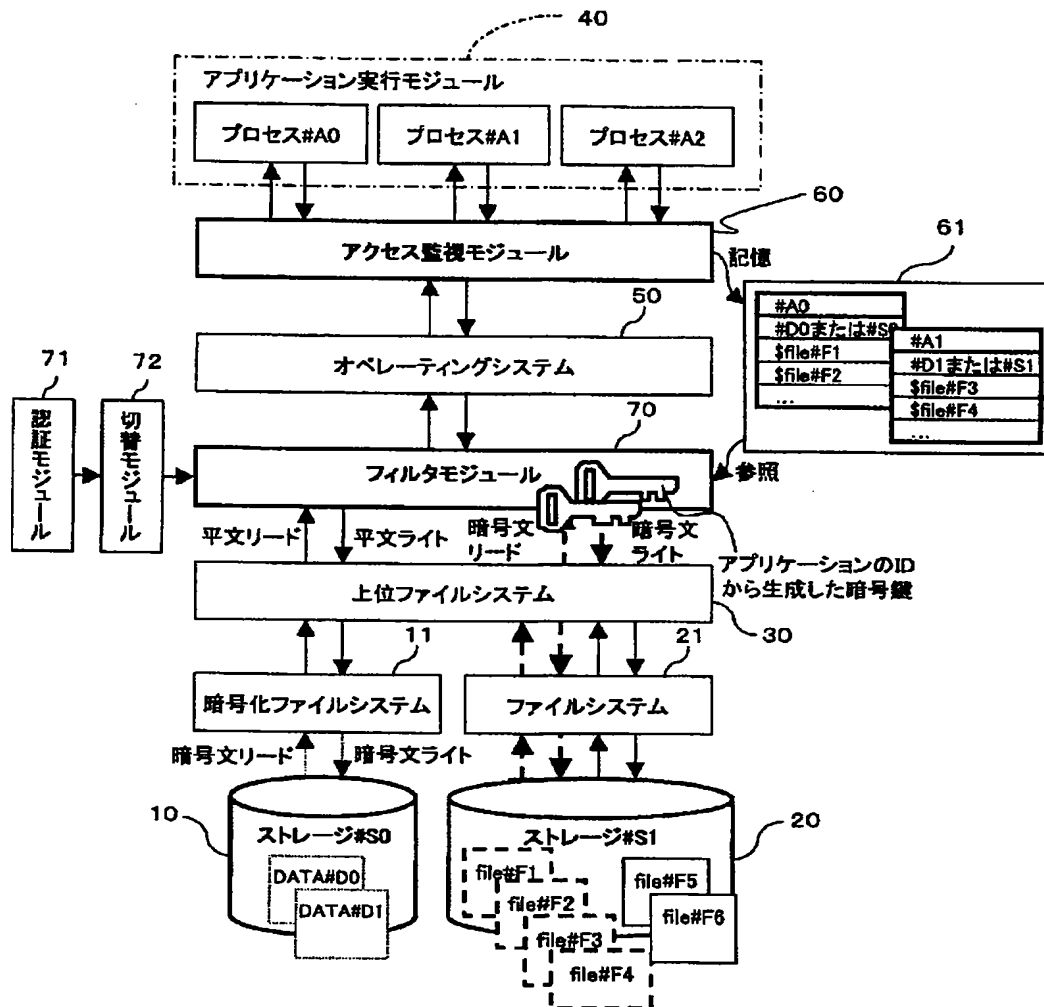
200 データ記録再生装置（第2蓄積装置）

300 データ記録再生装置（第1蓄積装置）

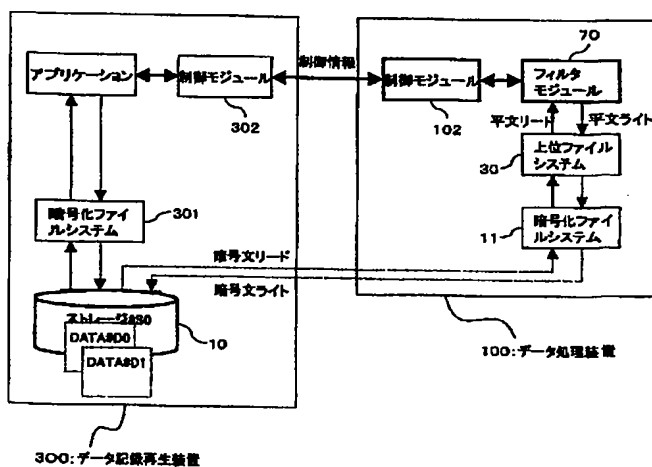
301 暗号化ファイルシステム

50 302 制御モジュール

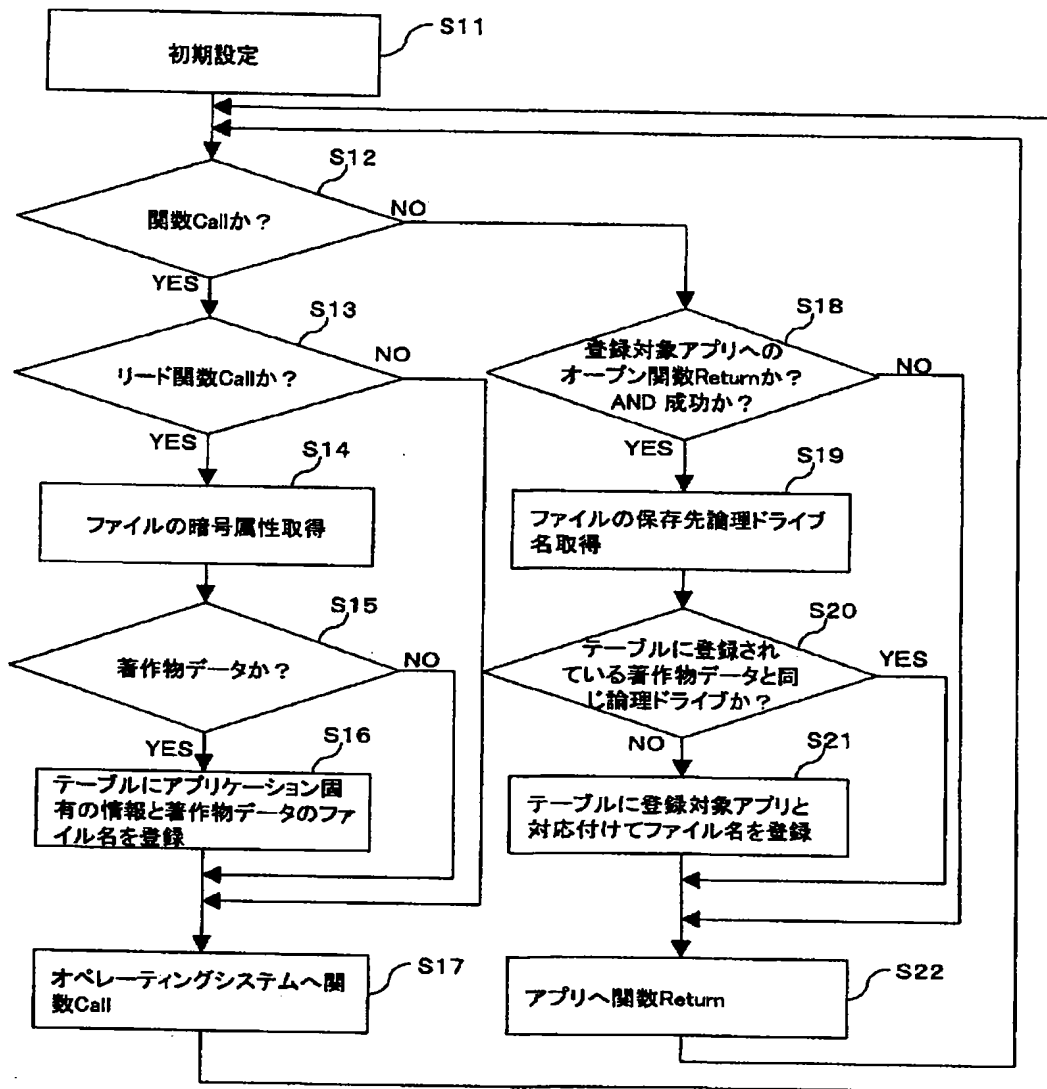
【図 1】



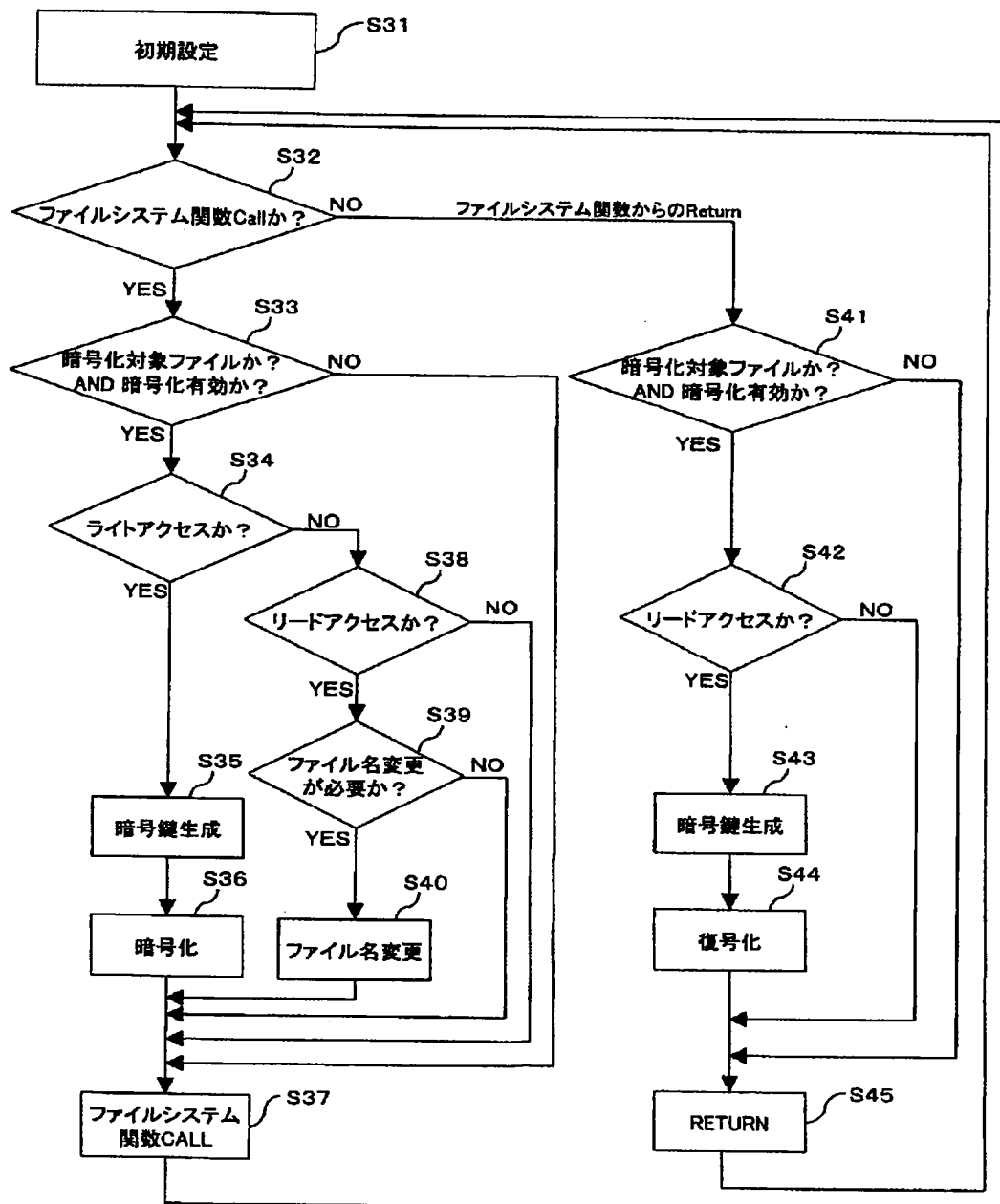
【図 7】



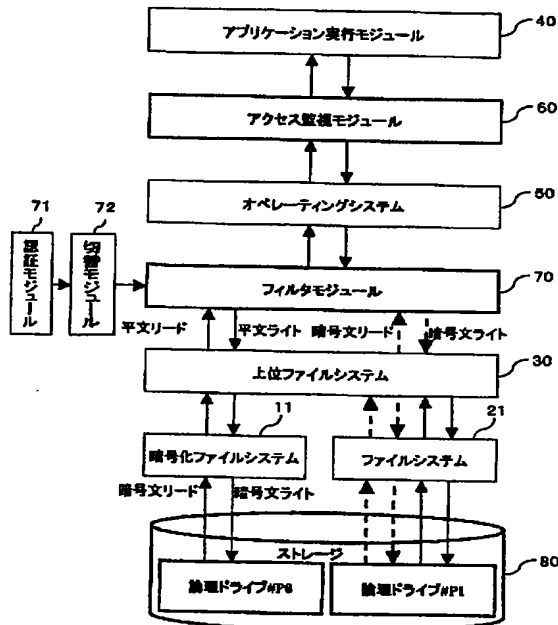
【図 2】



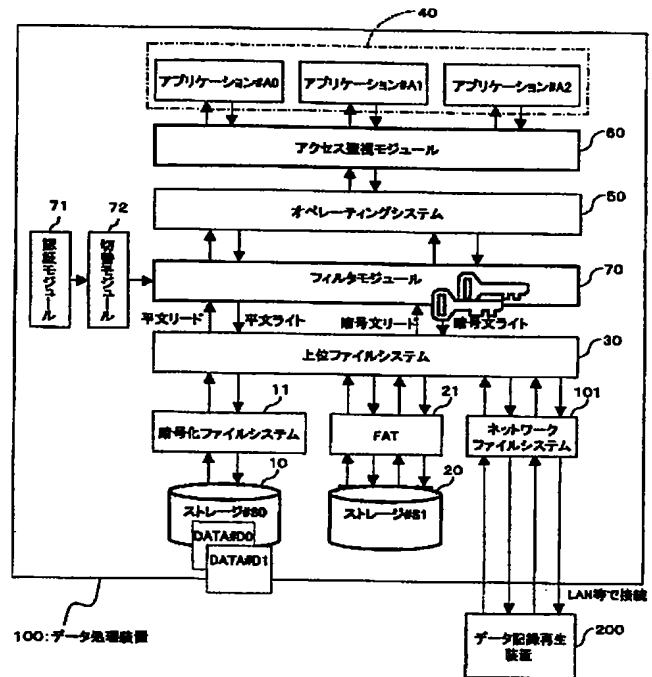
【図 3】



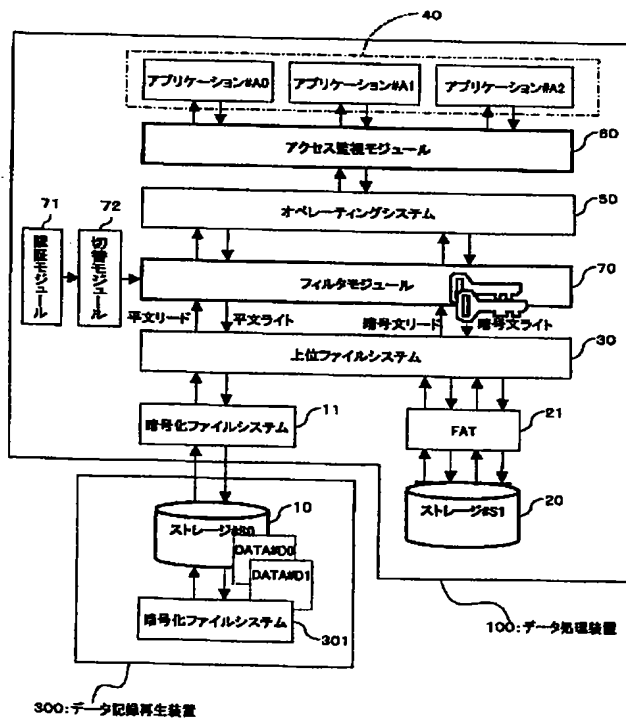
【図 4】



【図 5】



【図 6】



フロントページの続き

Fターム(参考) 5B017 AA03 AA06 BA07 BA09 CA07
CA16
5B082 EA11 GA00
5J104 AA01 PA14